App No.: 09/706,074

Title: Method and Apparatus for Protecting ...

Inventors: Michael O. Rabin et al.

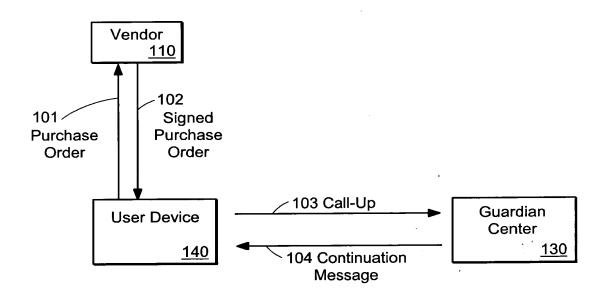


FIG. 1

Title: Method and Apparatus for Protecting ...

2/21

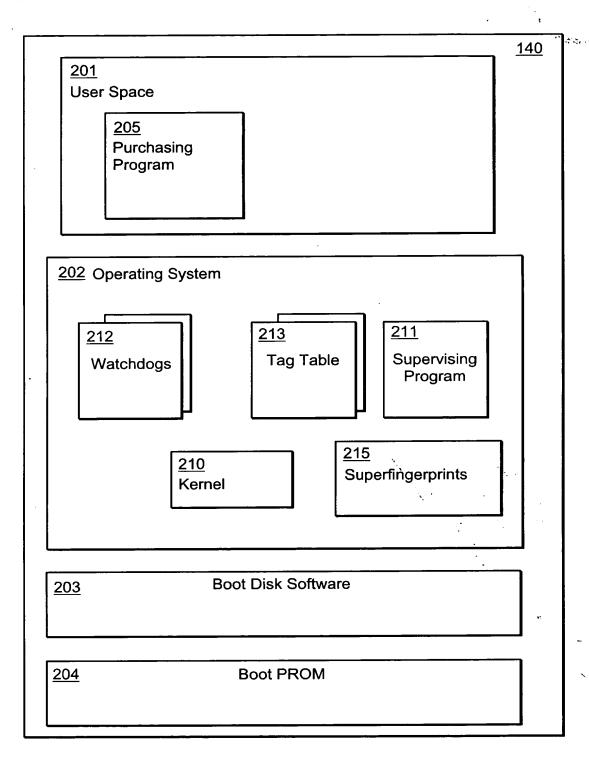


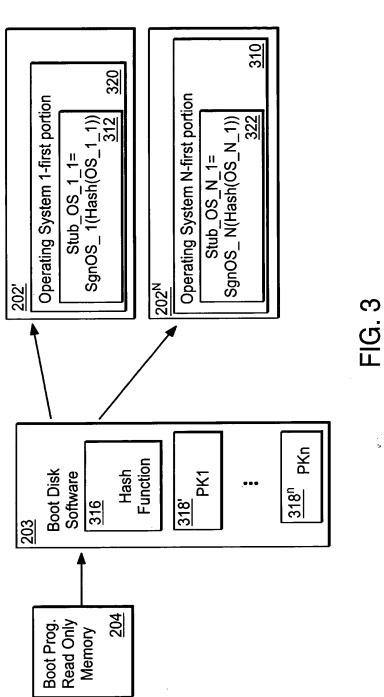
FIG. 2

App No.: 09/706,074

Title: Method and Apparatus for Protecting ...

Inventors: Michael O. Rabin et al.

3/21



Title: Method and Apparatus for Protecting ...

Michael O. Rabin et al. Inventors:

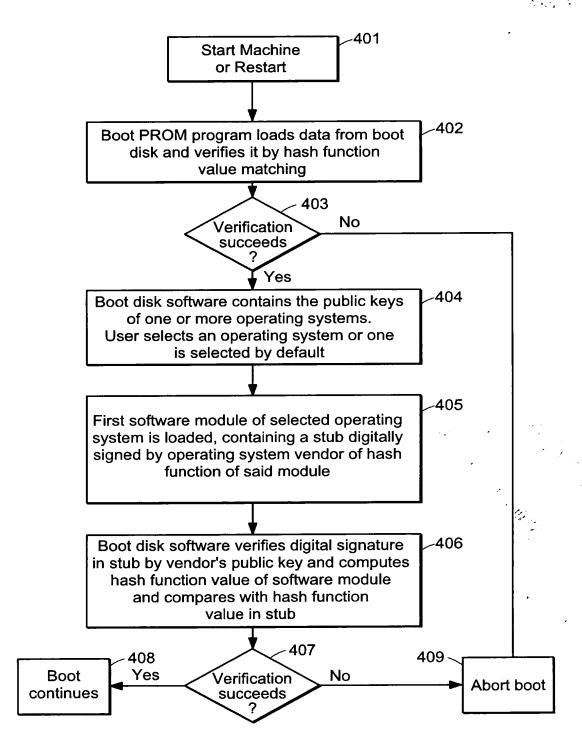


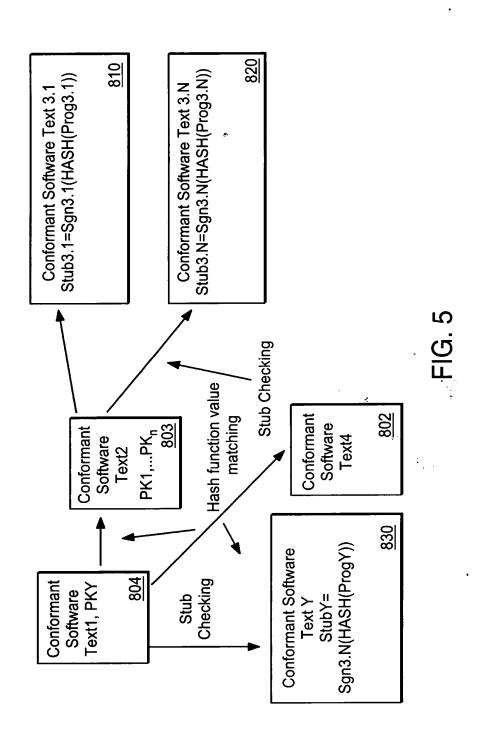
FIG. 4

App No.: 09/706,074

Title: Method and Apparatus for Protecting ...

Inventors: Michael O. Rabin et al.

5/21

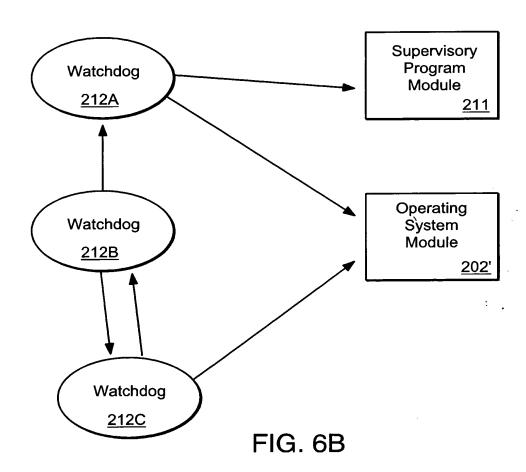


Title: Method and Apparatus for Protecting ...

6/21

530	
Watchdog Structure	
Optional need-to-check test	<u>532</u>
Addresses to be checked	<u>534</u>
Hash functions	<u>536</u>
Hash functions values	<u>538</u>
Watchdog actions	<u>540</u>

FIG. 6A



Title: Method and Apparatus for Protecting ...

Inventors: Michael O. Rabin et al.

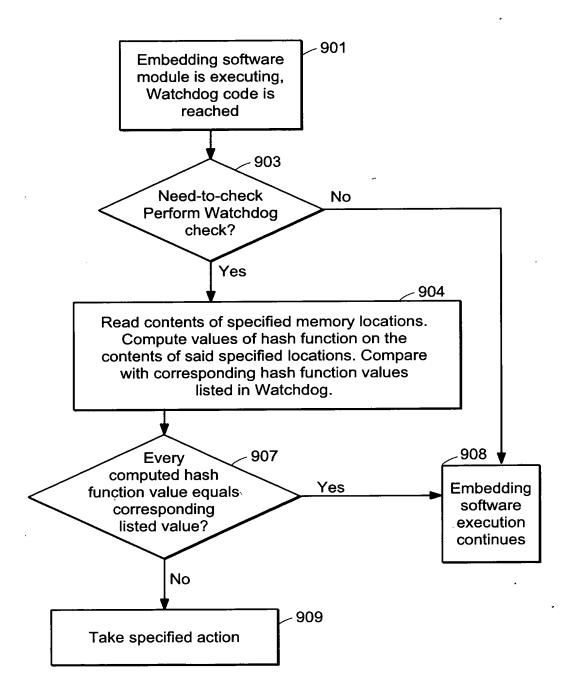


FIG. 6C

09/706,074 App No.:

Title: Method and Apparatus for Protecting ... Inventors: Michael O. Rabin et al.

8/21

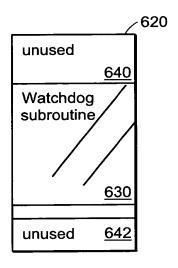


FIG. 6D

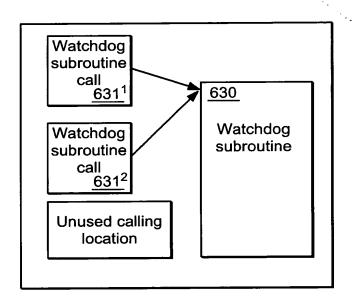


FIG. 6E

Title: Method and Apparatus for Protecting ...

Inventors: Michael O. Rabin et al.

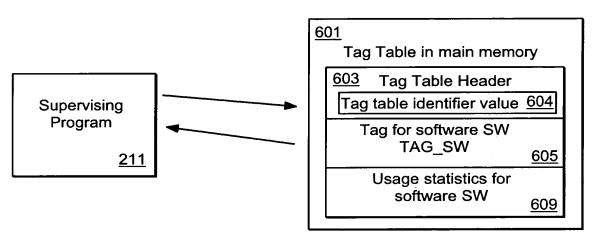
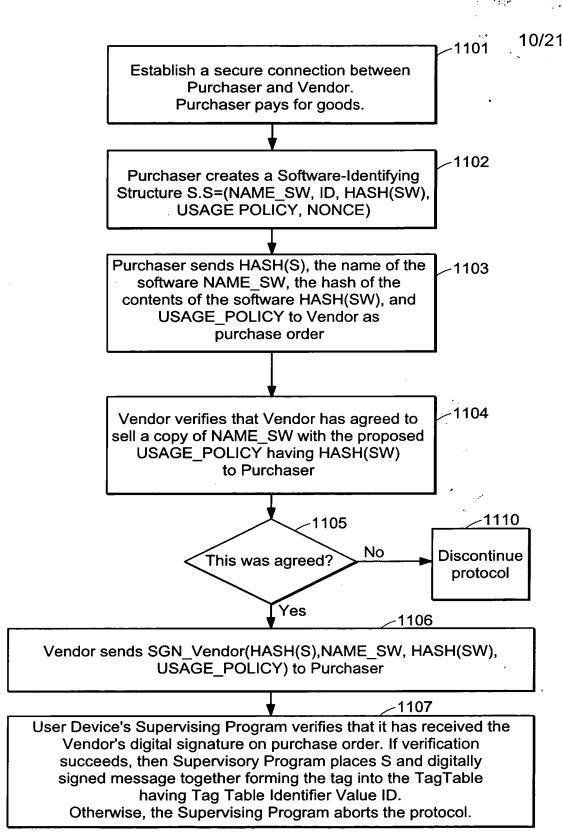


FIG. 7



App No.:

Inventors:

09/706,074 Title: Method and Apparatus for Protecting ... Michael O. Rabin et al.

FIG. 8

Title: Method and Apparatus for Protecting ...

Inventors: Michael O. Rabin et al.

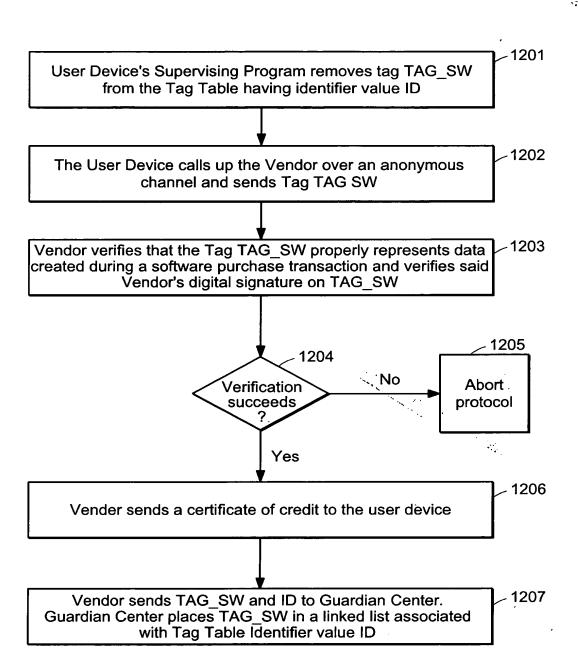
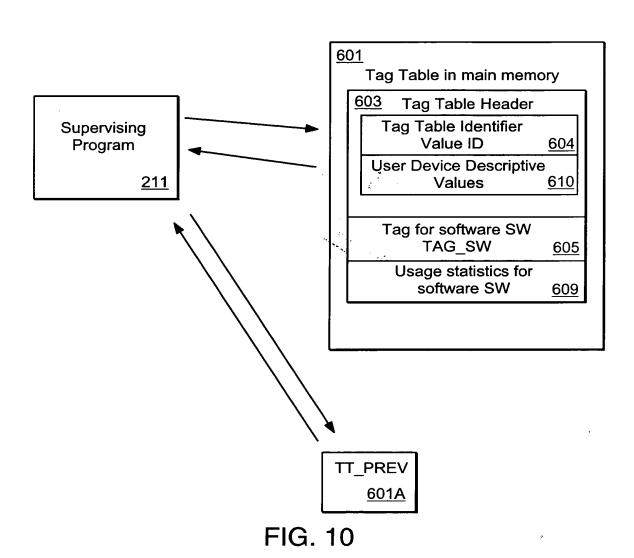


FIG. 9

Title: Method and Apparatus for Protecting ...

12/21



Title: Method and Apparatus for Protecting ...

Inventors: Michael O. Rabin et al.

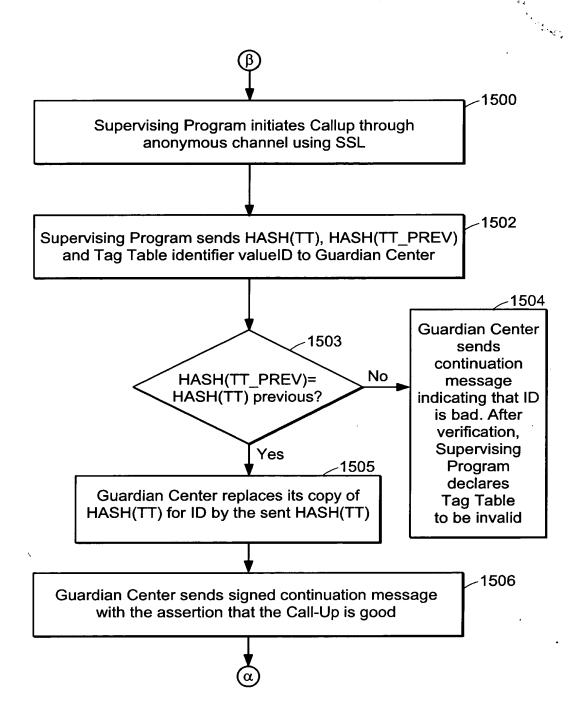


FIG. 11A

Title: Method and Apparatus for Protecting ...

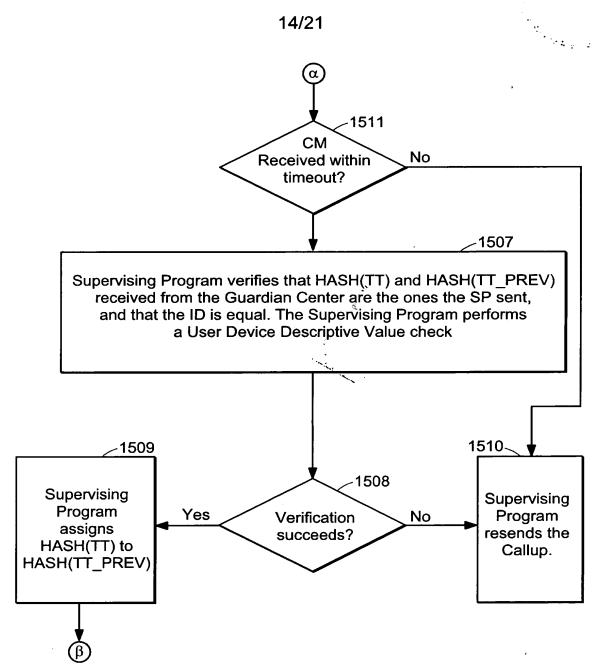


FIG. 11B

Title: Method and Apparatus for Protecting ...

Inventors: Michael O. Rabin et al.

15/21

-1000

Check the following conditions:

- 1) User Device Descriptive Values that are not expected to change in the time elapsed between two successive Call-Ups have changed.
- 2) User Device Descriptive Values that may change undergo the following changes: three previously sent Tag Tables have the property that the Header of the earliest sent Tag Table contains changeable UDDVs whose configuration of values is C, a subsequently sent Tag Table where the corresponding stored UDDVs have a markedly different configuration of values C_1, and a still later sent Tag Table where the corresponding stored UDDVs again have the configuration

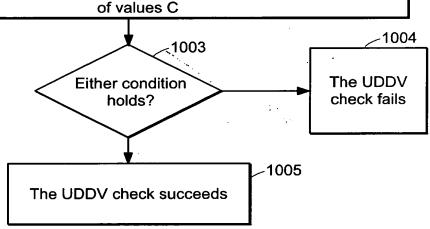
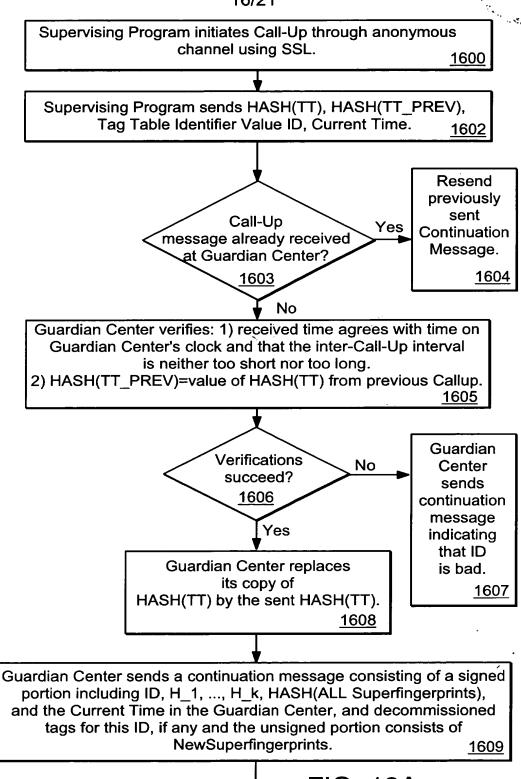


FIG. 12

Title: Method and Apparatus for Protecting ...

Inventors: Michael O. Rabin et al.

16/21



, FIG. 13A

Title: Method and Apparatus for Protecting ... Inventors: Michael O. Rabin et al.

17/21

9

Upon receiving the Continuation Message, Supervising Program verifies that HASH(TT)(=H_1) and HASH(TT_PREV)(=H_2) received from the Guardian Center are the ones the SP sent, and that the Tag Table Identifier Value ID is equal to the Tag Table Identifier Value associated with this Supervising Program. The Supervising Program further verifies that the hash function values of previous Tag Tables correspond to previously held Tag Tables in the User Device. The Supervising Program also performs a User Device Descriptive Value check.

The Supervising Program also verifies that the consumption recorded in the Tag Table sequence is non-decreasing in time. SP also verifies that decommissioned tags sent from the Guardian Center are absent from Tag Table. The Supervising Program also verifies that the NewSuperfingerprints sent and the ones already present on User Device are consistent with HASH(AllSuperfingerprints).

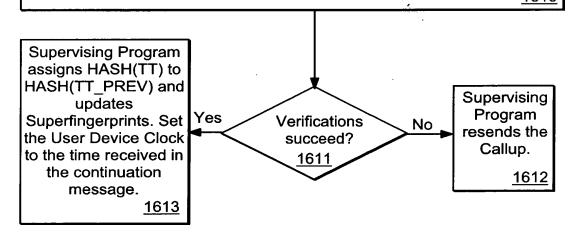


FIG. 13B

App No.: 09/706,074

Title: Method and Apparatus for Protecting ...

Inventors: Michael O. Rabin et al.

Inventors:

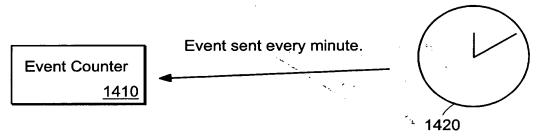


FIG. 14

Title: Method and Apparatus for Protecting ...

19/21

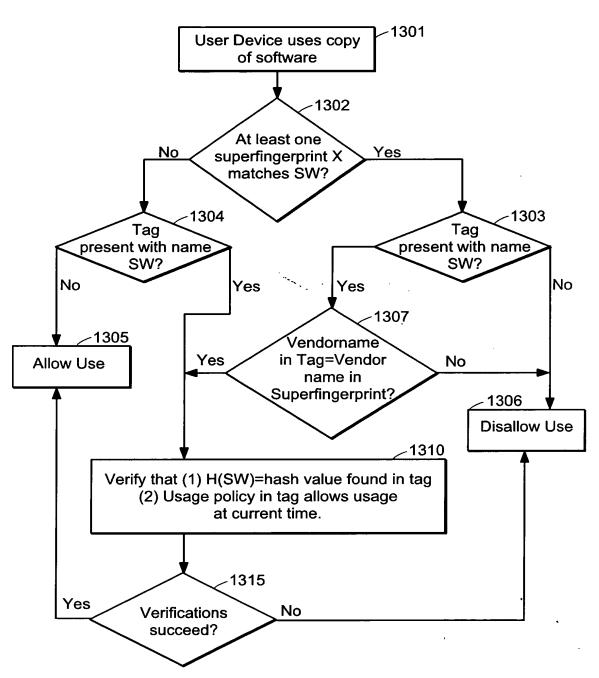


FIG. 15

Title: Method and Apparatus for Protecting ...

Inventors: Michael O. Rabin et al.

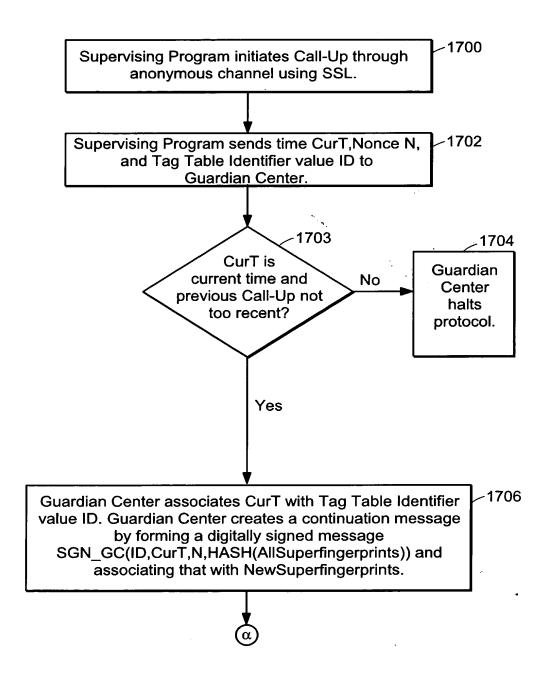


FIG. 16A

Title: Method and Apparatus for Protecting ...

Inventors: Michael O. Rabin et al.

21/21



Supervising Program verifies the digital signature of the Guardian Center received in the Continuation Message. The Supervising Program further verifies that the Tag Table Identifier value ID, the NONCE value N, and CurT received from the Guardian Center are equal to the corresponding values prepared by the Supervising Program for its Call-Up. The Supervising Program may optionally check that CurT is close to the time as recorded in the Supervising Program. Finally, the Supervising Program computes the hash function value of all its already received Superfingerprints, including the currently received NewSuperfingerprints, and verifies that the corresponding field in the Continuation Message equals the computed hash function value.

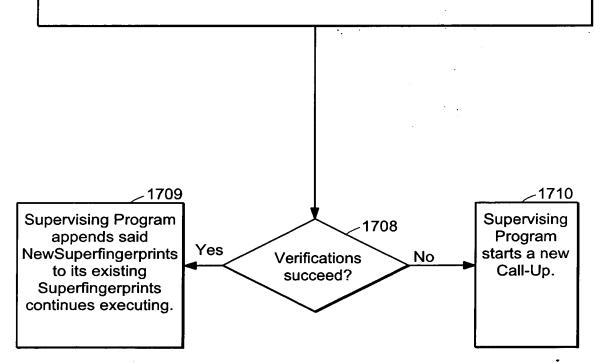


FIG. 16B